>>> "Hal Amens" <hal@lpf.com> 01/26/02 12:41PM >>>
The HIPAA Implementation Newsletter
Issue #26 - January 25, 2002
| Planning for October 2003 | Security | Quality |
Web format with links at http://lpf.com/hipaa

We have a favor to ask. Last week we crashed a hard disk. We have recovered
almost everything, but we lost the addresses of a few of our new subscribers. If you forwarded the newsletter to others recently, will you please forward it again? We want to include everyone. Thanks!

___Transactions: Planning for October 2003___

H.R. 3323 exempts providers and plans from the October 2002 compliance date
for transactions and code sets if, "before October 16, 2002, [they] submit to HHS a plan of how [they] will come into compliance with the requirements ... not later than October 16, 2003."

If you give a competent building contractor a set of architectural drawings, they can quickly develop a reliable estimate of the cost and time required to build a new building. No contractor in their right mind will give you anything more than a guess about the cost and time to remodel an existing building--there are just too many "unknowns." Getting transactions and code sets HIPAA compliant is a remodeling project that is full of potential unknowns.

What is needed to develop a "remodeling" plan for HIPAA compliance that your
organization can submit to HHS? Congress has directed the Secretary of HHS to promulgate a model form that can be used in drafting a plan. That will provide a format. The following material outlines what you need to do to develop the content.

1. As with any plan, you need a good description of the result you want to produce. That will include meeting the specific HIPAA regulations for transactions and code sets that are used by your organization.

2. A description of current systems and processes in sufficient detail that you will be able to reliably identify the elements that can be reused, modified, replaced or require further analysis. The systems and processes to be analyzed include: transaction data capture systems, transaction processing systems, data transmission; and the management and financial systems that will use information from the transactions. The objective of this step is development of information in sufficient detail to make

decisions and prepare plans.

3. A comparison of where you are and where you need to be, sometimes referred to as a "gap analysis." What is working that you can use in its present form? What can you modify to bring it to HIPAA compliance? What do
you have to replace? What needs further analysis before you can put it in one of these three categories? In addition to the systems and processes information developed in step 2, you will need a detailed analysis of current and required code sets. The "further analysis" category will include elements that may or may not lend themselves to modifications, new capabilities that do not appear to be candidates to add to existing systems or procedures, old systems and procedures that may need to be replaced for other reasons; and particularly those changes, development and management
tasks where you know you do not know enough to prepare a reliable plan.

The difficulty in identifying what is "unknown" and getting the information that needs to be know is what creates the analogy to a remodeling project. Sometimes you need to take things apart and examine them in detail to determine what needs to be done and how long that will take.

4. A strategic context for the project. What else do you know or what is reasonably predictable that should be considered in developing the plan? Examples include possible regulatory changes such as computer prescription order entry (the types of items often referred to in this newsletter under the heading: It's not just HIPAA), changes in our operating environment such as mergers and reorganizations (yours or other organizations in your marketplace,) and the availability of resources including skills, money and time. The additional time may allow additional changes to be included in the project to improve performance or return on investment.

5. An organizational strategy to design and manage what needs to be done. Who is responsible for what? How will plans and progress be tracked and by whom? How will development and operational organizations interact? How will
the required interactions be scheduled, managed and evaluated; how will you know when they have accomplished what needs to be done? How will resources
be allocated, both money and time?

By now, most organizations have started this process. If you have started, this is a good time to conduct a quick audit to assure that you have the information you need to develop a reliable plan that can be deliver to HHS by October 2002 and completed on or before October 2003. The deadline has moved. Is your organization taking full advantage of the extra time to improve the return on your investment? Do you have the information you need

to develop a plan that will survive outside scrutiny?

6. Develop or modify your near term plans give top priority to:

* Resolution of open issues for the tasks where you know you do not know enough to prepare a reliable plan. If the required development or modifications are significant, these tasks will probably lay one the "critical path" for your project and have a major impact on the ability to meet the new October 16, 2003 date. "We didn't know" is not an excuse if you could have known but chose not to look.

* Items with the best cost/benefit ratio. HIPAA transactions and code sets are an investment and should be managed to maximize the return on that investment. In Issue #22, we presented guidelines for sequencing the implementation of transactions and code sets that may be useful. http://lpf.com/hipaa/issue22.html#transactions-sequence-22

7. Use what you accomplish, and more important, what you learn over the next few months to develop the plan for compliance. Said another way, continue (or start) your remodeling and use the next few months to learn more about current systems and procedures as a basis for better planning.

All of the articles we have published related to transactions and code sets have been consolidated in a topic paper: HIPAA Transactions. http://lpf.com/hipaa/t-transactions.html You can also use the right hand column on the Past Issues page to find articles about transactions and related information. http://lpf.com/hipaa/past.html

___Security: Contingency Planning___

The National Institute of Standards and Technology has released a draft "Contingency Planning Guide for Information Technology Systems." This was developed with federal funding. We would not be surprised if some or all of this guide appears as part of the pending security regulations for HIPAA. The guide is IT focused and deals with: desktops and portable systems, Web sites, servers, local area networks, wide area networks, distributed systems, and mainframe systems. HIPAA contingency plans will also have to deal with the administrative and clinical impact of a failure. Ninety-four pages in pdf format. http://csrc.ncsl.nist.gov/publications/drafts/ITcontingency-planning-guideline.pdf

___Security: Firewalls___

The National Institute of Standards and Technology has also released "Guidelines on Firewalls and Firewall Policy." "This document provides

introductory information about firewalls and firewall policy primarily to assist those responsible for network security. It addresses concepts relating to the design, selection, deployment, and management of firewalls and firewall environments. This document is not intended to provide a mandatory framework for firewalls and firewall environments, but rather to present suggested approaches to the topic." Seventy-four pages in PDF format.
http://csrc.ncsl.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

___Security: OCTAVE Method___

OCTAVE(sm) is a method to, "identify and manage enterprise-wide information
security risks and develop appropriate protection strategies by considering policy, management, administrative, technological, and other issues to form a comprehensive view of the security state of your organization." It was developed by the Software Engineering Institute at Carnegie Mellon University under a government contract. The primary documents -- Practices, Criteria and Implementation Guide -- are now at version 2, dated December 2001.

"The catalog of practices is a general catalog; it is not specific to any domain, organization, or set of regulations. It can be modified to suit a particular domain's standard of due care or set of regulations (e.g., the medical community and Health Insurance Portability and Accountability Act [HIPAA] security regulations). It can also be extended to add organization-specific standards, "... [Page 17]

Octave is designed to be used for organizational self-assessment. Based on our reading, it also provides a good checklist for high level planning for either self-assessment or outsourcing. If you chose to outsource, it provides a basis for the evaluation of proposed vendor work plans. Introductory material and links are at: http://www.cert.org/octave/

Again, this was developed with federal money and it specifically cites HIPAA as a possible application. We would not be surprised to see it or portions of it in the pending security regulations.

We have added a link to Octave from the "privacy-security" page
http://lpf.com/hipaa/privacy-security.html#security-tools
http://www.cert.org/octave/

___Security: Microsoft___

Significant portions of the computer power of most organizations resides on PCs that use
Microsoft products. Security vulnerability in any Microsoft product creates a potential threat to the PCs using that software and other devices to which

it is networked.

An article in the January 22, 2002, Los Angeles Times reported that, "Microsoft Corp. may delay some products, including its next version of Windows for server computers, to improve security, Vice President Cliff Reeves said Monday. About 7,000 engineers in the Windows operating system,
word-processing and e-mail product groups are in security training..."

Microsoft has a security notification service. "This is a free e-mail notification service that Microsoft uses to send information to subscribers about the security of Microsoft products. Anyone can subscribe to the service, and you can unsubscribe at any time." You may find this useful in keeping security current for you Microsoft products.

http://latimes.com/business/la-000005547jan22.story?coll=la%2Dheadlines%2Dbu
siness
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/
bulletin/notify.asp

___It's Not Just HIPAA: A Shift to Quality___

A recent article in the Los Angeles Times reported, " Aetna Inc., Blue Cross of California, Blue Shield of California, Cigna Corp., Health Net Inc. and PacifiCare Health Systems Inc., have agreed on a common set of standards for
measuring performance under which doctors and hospitals will be rewarded with bonuses of at least 5% of the billed amounts for providing quality health care and for avoiding medical errors.

"Meanwhile, beginning later this month, the New York-based employees of some
of the nation's largest companies, including IBM Corp., Xerox Corp., Verizon Communications and PepsiCo Inc., will be able to access a Web site that contains the beginnings of another new approach to health care: information on which of nearly 150 hospitals in the area have the most experience and the best outcomes on a variety of surgical procedures."

It is becoming predictable that information that will be made available as a result of the standardization of transactions and code sets will be used and combined with additional data in ways we are only beginning to see on the horizon. Build flexibility into your systems.
http://latimes.com/business/la-000003459jan14.story?coll=la%2Dheadlines%2Dbu
siness

___Update___

We have added: Privacy and security guidelines from the Association of American Medical Colleges to the privacy-security page
http://www.aamc.org
WEDI has published version 2 of Business Business-to-Business Transaction Set Testing. We have updated the link in Issue #22.
http://snip.wedi.org/public/articles/bus2bustestv02.pdf

_____

To subscribe, click: mailto:hipaa@lpf.com?subject=subscribe We appreciate it
if you include information about your firm and your interests.

 Issues are posted on
the Web at http://lpf.com/hipaa concurrent with email distribution. Past issues are also available there. Edited by Hal Amens hal@lpf.com

Information in the HIPAA Implementation newsletter is based on our experience as management consultants and sources we consider reliable. There
are no further warranties about accuracy or applicability. It contains neither legal nor financial advice. For that, consult appropriate professionals.

Lyon, Popanz & Forester http://lpf.com is a management-consulting firm that designs and manages projects that solve management problems. Planning, program management offices and project management for HIPAA are areas of
special interest.